# Elhady Plaintiffs
# MSJ Exhibit 41

**United States Government Accountability Office**

GAO

Statement for the Record
To the Committee on Homeland Security,
House of Representatives

For Release on Delivery
Expected on Wednesday,
January 27, 2010

# HOMELAND SECURITY

# Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security

Statement for the Record by Eileen R. Larence
Director, Homeland Security and Justice Issues

and

Stephen M. Lord
Director, Homeland Security and Justice Issues

January 27, 2010

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-10-401T, a statement for the record to the Committee on Homeland Security, House of Representatives

# HOMELAND SECURITY

## Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Checkpoint Technologies Could Further Strengthen Security

### Why GAO Did This Study

The December 25, 2009, attempted bombing of flight 253 raised questions about the federal government's ability to protect the homeland and secure the commercial aviation system. This statement focuses on the government's efforts to use the terrorist watchlist to screen individuals and determine if they pose a threat, and how failures in this process contributed to the December 25 attempted attack. This statement also addresses the Transportation Security Administration's (TSA) planned deployment of technologies for enhanced explosive detection and the challenges associated with this deployment. GAO's comments are based on products issued from September 2006 through October 2009 and selected updates in January 2010. For these updates, GAO reviewed government reports related to the December 25 attempted attack and obtained information from the Department of Homeland Security (DHS) and TSA on use of the watchlist and new technologies for screening airline passengers.

### What GAO Recommends

GAO is not making new recommendations, but has made recommendations in prior reports to DHS, the Federal Bureau of Investigation (FBI), and the White House Homeland Security Council to enhance the use of the watchlist and to TSA related to checkpoint technologies. The agencies generally agreed and are making some progress, but full implementation is needed.

View GAO-10-401T or key components. For more information, contact Eileen Larence at (202) 512-6510 or larencee@gao.gov and Stephen Lord at (202) 512-4379 or lords@gao.gov.

### What GAO Found

The intelligence community uses standards of reasonableness to evaluate individuals for nomination to the consolidated terrorist watchlist. In making these determinations, agencies are to consider information from all available sources. However, for the December 25 subject, the intelligence community did not effectively complete these steps and link available information to the subject before the incident. Therefore, agencies did not nominate the individual to the watchlist or any of the subset lists used during agency screening, such as the "No Fly" list. Weighing and responding to the potential impacts that changes to the nomination criteria would have on the traveling public will be an important consideration in determining what changes may be needed. Also, screening agencies stated that they do not check against all records in the watchlist, partly because screening against certain records may not be needed to support a respective agency's mission or may not be possible because of the requirements of computer programs used to check individuals against watchlist records. In October 2007, GAO reported that not checking against all records may pose a security risk and recommended that DHS and the FBI assess potential vulnerabilities, but they have not completed these assessments. TSA is implementing an advanced airline passenger prescreening program—known as Secure Flight—that could potentially result in the federal government checking passengers against the entire watchlist under certain security conditions. Further, the government lacks an up-to-date strategy and implementation plan—supported by a clearly defined leadership or governance structure—which are needed to enhance the effectiveness of terrorist-related screening and ensure accountability. In the 2007 report, GAO recommended that the Homeland Security Council ensure that a governance structure exists that has the requisite authority over the watchlist process. The council did not comment on this recommendation.

As GAO reported in October 2009, since TSA's creation, 10 passenger screening technologies have been in various phases of research, development, procurement, and deployment, including the Advanced Imaging Technology (AIT)—formerly known as the Whole Body Imager. TSA expects to have installed almost 200 AITs in airports by the end of calendar year 2010 and plans to install a total of 878 units by the end of fiscal year 2014. In October 2009, GAO reported that TSA had not yet conducted an assessment of the technology's vulnerabilities to determine the extent to which a terrorist could employ tactics that would evade detection by the AIT. Thus, it is unclear whether the AIT or other technologies would have detected the weapon used in the December 25 attempted attack. GAO's report also noted the problems TSA experienced in deploying another checkpoint technology that had not been tested in the operational environment. Since GAO's October report, TSA stated that it has completed the testing as of the end of 2009. We are currently verifying that all functional requirements of the AIT were tested in an operational environment. Completing these steps should better position TSA to ensure that its costly deployment of AIT machines will enhance passenger checkpoint security.

Mr. Chairman and Members of the Committee:

We are pleased to submit this statement on the progress federal agencies have made and the challenges they face in key areas of terrorism information sharing and the deployment of checkpoint technologies. The December 25, 2009, attempted bombing of flight 253 has led to increased scrutiny of how the government creates and uses the consolidated terrorist screening database (the watchlist) to screen individuals and determine if they pose a security threat, and highlighted the importance of detecting improvised explosive devices and other prohibited items on passengers before they board a commercial aircraft. The White House's initial review of these events exposed gaps in how intelligence agencies collected, shared, and analyzed terrorism-related information to determine if the subject—Umar Farouk Abdulmutallab—posed enough of a threat to warrant placing him on the watchlist, which could have altered the course of events that day. To enhance its ability to detect explosive devices and other prohibited items on passengers, the Transportation Security Administration (TSA) is evaluating the use of Advanced Imaging Technology (AIT)—formerly called the Whole Body Imager—as an improvement over current screening capabilities.

In October 2007, we released a report on the results of our review—conducted at your request—of how the watchlist is created and maintained, and how federal, state, and local security partners use the list to screen individuals for potential threats to the homeland.[1] As a result of that review, we identified potential vulnerabilities, including ones created because agencies were not screening against all records in the watchlist. We made a number of recommendations aimed at addressing these potential vulnerabilities and helping to enhance the effectiveness of the watchlist process, which the agencies have not yet fully addressed. These recommendations—which we discuss later in this statement—are still important to address and can inform ongoing reviews of the December 25 attempted terrorist attack.

Also, in January 2005, we designated information sharing for homeland security a high-risk area because the government faced formidable challenges in analyzing and disseminating this information in a timely,

[1]GAO, *Terrorist Watchlist Screening: Opportunities Exist to Enhance Management Oversight, Reduce Vulnerabilities in Agency Screening Processes, and Expand Use of the List*, GAO-08-110 (Washington, D.C.: Oct. 11, 2007).

accurate, and useful manner.[2] Since then, we have been monitoring and making recommendations to improve the government's efforts to share terrorism-related information, not only among federal agencies but also with their state, local, tribal, and private sector security partners.[3] Addressing this high-risk area is important to help remove barriers that lead to agencies maintaining information in stove-piped systems, and to hold them accountable to the Congress and the public for ensuring terrorism information is shared, is used, and makes a difference. We are continuing to review federal agencies' efforts to share terrorism-related information and expect to report the results of this work later this year.[4]

In addition, in October 2009, we released a report on TSA's efforts to deploy checkpoint technologies and the challenges the agency faces in these efforts.[5] We made eight recommendations related to the research, development, and deployment of these technologies. The Department of Homeland Security (DHS) agreed with our recommendations and identified actions planned or under way to implement them. While DHS is taking steps to address our recommendations related to conducting risk assessments, the actions DHS reported that TSA had taken or plans to take do not fully address the intent of the majority of our recommendations.

This statement for the record discusses (1) the government's efforts to use the terrorist watchlist to screen individuals and determine if they pose a threat, as well as how aspects of this process contributed to the December 25 attempted terrorist attack and (2) TSA's planned deployment of the AIT

[2]See GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009), for our most recent update.

[3]See, for example, GAO, *Information Sharing: The Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information*, GAO-06-385 (Washington, D.C.: Mar. 17, 2006); *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GAO-08-492 (Washington, D.C.: June 25, 2008); and *Information Sharing: Federal Agencies Are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts Are Needed*, GAO-10-41 (Washington, D.C.: Dec. 18, 2009).

[4]We have three ongoing reviews of terrorism-related information sharing that are being conducted based on separate requests from your committee, the House Committee on Oversight and Government Reform, and the Senate Committee on Homeland Security and Governmental Affairs.

[5]GAO, *Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face* Challenges, GAO-10-128 (Washington, D.C.: Oct. 7, 2009).

for enhanced explosive detection and the challenges associated with this deployment.

This statement is based on products GAO issued from September 2006 through October 2009.[6] In conducting our prior work, we reviewed documentation obtained from and interviewed officials at the various departments and agencies with responsibilities for compiling and using watchlist records. We also reviewed documentation and obtained information on current checkpoint screening technologies being researched, developed, and deployed. Our previously published reports contain additional details on the scope and methodology for those reviews. In addition, this statement contains selected updates conducted in December 2009 and January 2010. For the updates, GAO reviewed government reports and other information related to the December 25 attempted attack, obtained information from DHS and TSA on the use of watchlist records and new technologies for screening airline passengers, and interviewed a senior TSA official. We conducted our updated work in December 2009 and January 2010 in accordance with generally accepted government auditing standards.

## In Summary

Because the subject of the December 25 attempted terrorist attack was not nominated for inclusion on the government's consolidated terrorist screening database, federal agencies responsible for screening activities missed several opportunities to identify him and possibly take action. We have previously reported on a number of issues related to the compilation and use of watchlist records, such as the potential security risk posed by not checking against all records on the watchlist. We also identified the need for an up-to-date strategy and implementation plan—one that describes the scope, governance, outcomes, milestones, and metrics, among other things—for managing the watchlist process across the federal government. Such a strategy and plan, supported by a clearly defined leadership or governance structure, can be helpful in removing cultural, technological, and other barriers—such as those problems that the December 25 attempted terrorist attack exposed—that inhibit the effective use of watchlist information.

[6]See GAO, *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*, GAO-06-1031 (Washington, D.C.: Sept. 29, 2006); GAO-08-110; *Aviation Security: TSA Has Completed Key Activities Associated with Implementing Secure Flight, but Additional Actions Are Needed to Mitigate Risks*, GAO-09-292 (Washington, D.C.: May 13, 2009); and GAO-10-128.

With regard to the deployment of technology to detect explosives on passengers, TSA expects to have installed almost 200 AITs in airports by the end of calendar year 2010, and plans to procure and install a total of 878 units by the end of fiscal year 2014. While recently providing GAO with updated information to our October 2009 report, TSA stated that operational testing for the AIT was completed as of the end of calendar year 2009. We are in the process of verifying that TSA tested all of the AIT functional requirements in an operational environment. Moreover, we previously reported that TSA had not yet conducted an assessment of the technology's vulnerabilities to determine the extent to which a terrorist could employ tactics that would evade detection by the AIT. While we recognize that the AIT could provide an enhanced detection capability, completing these steps should better position TSA to have the information necessary to ensure that moving ahead with a costly deployment of AIT machines will enhance passenger checkpoint security.

# Background

## Terrorist Watchlist Process

The Terrorist Screening Center (TSC)—administered by the Federal Bureau of Investigation (FBI)—is responsible for maintaining the U.S. government's consolidated watchlist and providing it to federal agencies as well as state, local, and selected foreign partners for their use in screening individuals. TSC receives the vast majority of its watchlist nominations and information from the National Counterterrorism Center (NCTC), which compiles information on known or suspected international terrorists from executive branch departments and agencies.[7] In addition, the FBI provides TSC with information on known or suspected domestic terrorists who operate primarily within the United States. To support agency screening processes, TSC first determines if each nomination contains specific minimum derogatory information for inclusion in its terrorist screening database. TSC then sends applicable records from the terrorist watchlist to screening agency systems for use in efforts to deter or detect the movements of known or suspected terrorists. For instance, applicable TSC records are provided to TSA for use in prescreening airline

[7]By law, NCTC, which is within the Office of the Director of National Intelligence, serves as the primary organization in the U.S. government for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism, except for intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism. See 50 U.S.C. § 404o(d)(1).

passengers; to a U.S. Customs and Border Protection (CBP) system for use in screening travelers entering the United States; to a Department of State system for use in screening visa applicants; and to an FBI system for use by state and local law enforcement agencies pursuant to arrests, detentions, and other criminal justice purposes.[8]

## Airline Passenger Screening Using Checkpoint Screening Technology

Passenger screening is a process by which screeners inspect individuals and their property to deter and prevent an act of violence or air piracy, such as the carrying of any unauthorized explosive, incendiary, weapon, or other prohibited item on board an aircraft or into a sterile area.[9] Screeners inspect individuals for prohibited items at designated screening locations. TSA developed standard operating procedures for screening passengers at airport checkpoints. Primary screening is conducted on all airline passengers before they enter the sterile area of an airport and involves passengers walking through a metal detector and carry-on items being subjected to X-ray screening. Passengers who alarm the walk-through metal detector or are designated as selectees—that is, passengers selected for additional screening—must then undergo secondary screening, as well as passengers whose carry-on items have been identified by the X-ray machine as potentially containing prohibited items.[10] Secondary screening involves additional means for screening passengers, such as by hand-wand; physical pat-down; or, at certain airport locations, an explosives trace portal (ETP), which is used to detect traces of explosives on passengers by using puffs of air to dislodge particles from their bodies and clothing into an analyzer. Selectees' carry-on items are also physically searched or screened for explosives, such as by using explosives trace detection machines.

[8]See GAO-08-110 for additional details on the compilation and use of terrorist watchlist records.

[9]Sterile areas are generally located within the terminal where passengers are provided access to boarding aircraft, and access is controlled in accordance with TSA requirements.

[10]A nonselectee passenger who alarms the walk-through metal detector on the first pass is offered a second pass. If the passenger declines the second pass, the passenger must proceed to additional screening. If the nonselectee passenger accepts the second pass and the machine does not alarm, the passenger may generally proceed without further screening.

## Assessing Potential Vulnerabilities Related to Not Screening against All Watchlist Records and Ensuring Clear Lines of Authority over the Watchlist Process Would Provide for Its More Effective Use

### Agencies Rely upon Standards of Reasonableness in Assessing Individuals for Nomination to TSC's Watchlist, but Did Not Connect Available Information on Mr. Abdulmutallab to Determine Whether a Reasonable Suspicion Existed

Federal agencies—particularly NCTC and the FBI—submit to TSC nominations of individuals to be included on the consolidated watchlist. For example, NCTC receives terrorist-related information from executive branch departments and agencies, such as the Department of State, the Central Intelligence Agency, and the FBI, and catalogs this information in its Terrorist Identities Datamart Environment database, commonly known as the TIDE database. This database serves as the U.S. government's central classified database with information on known or suspected international terrorists. According to NCTC, agencies submit watchlist nomination reports to the center, but are not required to specify individual screening systems that they believe should receive the watchlist record, such as the No Fly list of individuals who are to be denied boarding an aircraft.[11] NCTC is to presume that agency nominations are valid unless it has other information in its possession to rebut that position.

To decide if a person poses enough of a threat to be placed on the watchlist, agencies are to follow Homeland Security Presidential Directive (HSPD) 6, which states that the watchlist is to contain information about individuals "known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to

[11]As discussed later in this statement, agencies generally do not use the full terrorist watchlist to screen individuals. Rather, they generally use subsets of the full list based on each agency's mission and other factors.

terrorism."[12] HSPD-24 definitively established the "reasonable suspicion" standard for watchlisting by providing that agencies are to make available to other agencies all biometric information associated with "persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security."[13] NCTC is to consider information from all available sources and databases to determine if there is a reasonable suspicion of links to terrorism that warrants a nomination, which can involve some level of subjectivity. The guidance on determining reasonable suspicion, which TSC most recently updated in February 2009, contains specific examples of the types of terrorism-related conduct that may make an individual appropriate for inclusion on the watchlist.

The White House's review of the December 25 attempted terrorist attack noted that Mr. Abdulmutallab's father met with U.S. Embassy officers in Abuja, Nigeria, to discuss his concerns that his son may have come under the influence of unidentified extremists and had planned to travel to Yemen.[14] However, according to NCTC, the information in the State Department's nomination report did not meet the criteria for watchlisting in TSC's consolidated terrorist screening database per the government's established and approved nomination standards. NCTC also noted that the State Department cable nominating Mr. Abdulmutallab had no indication that the father was the source of the information. According to the White House review of the December 25 attempted attack, the U.S. government had sufficient information to have uncovered and potentially disrupted the attack—including by placing Mr. Abdulmutallab on the No Fly list—but analysts within the intelligence community failed to connect the dots that could have identified and warned of the specific threat.

After receiving the results of the White House's review of the December 25 attempted attack, the President called for members of the intelligence community to undertake a number of corrective actions—such as clarifying intelligence agency roles, responsibilities, and accountabilities to document, share, and analyze all sources of intelligence and threat

[12]The White House, *Homeland Security Presidential Directive/HSPD-6, Subject: Integration and Use of Screening Information* (Washington, D.C., Sept. 16, 2003).

[13]The White House, *Homeland Security Presidential Directive/HSPD-24, Subject: Biometrics for Identification and Screening to Enhance National Security* (Washington, D.C., June 5, 2008).

[14]The White House, *Summary of the White House Review of the December 25, 2009, Attempted Terrorist Attack* (Washington, D.C., Jan. 7, 2010).

threads related to terrorism, and accelerating information technology enhancements that will help with information correlation and analysis. The House Committee on Oversight and Government Reform has asked us, among other things, to assess government efforts to revise the watchlist process, including actions taken related to the December 25 attempted attack.

As part of our monitoring of high-risk issues, we also have ongoing work—at the request of the Senate Committee on Homeland Security and Governmental Affairs—that is assessing agency efforts to create the Information Sharing Environment, which is intended to break down barriers to sharing terrorism-related information, especially across federal agencies.[15] Our work is designed to help ensure that federal agencies have a road map that defines roles, responsibilities, actions, and time frames for removing barriers, as well as a system to hold agencies accountable to the Congress and the public for making progress on these efforts. Among other things, this road map can be helpful in removing cultural, technological, and other barriers that lead to agencies maintaining information in stove-piped systems so that it is not easily accessible, similar to those problems that the December 25 attempted attack exposed. We expect to issue the results of this work later this year.

## By Not Placing Mr. Abdulmutallab on the Consolidated Watchlist or Its Subsets, the Government Missed Opportunities to Use These Counterterrorism Tools

Following the December 25 attempted terrorist attack, questions were raised as to what could have happened if Mr. Abdulmutallab had been on TSC's consolidated terrorist screening database. We created several scenarios to help explain how the watchlist process is intended to work and what opportunities agencies could have had to identify him if he was on the watchlist. For example, according to TSC, if a record from the terrorist screening database is sent to the State Department's system and the individual in that record holds a valid visa, TSC would compare the identifying information in the watchlist record against identifying information in the visa and forward positive matches to the State Department for possible visa revocation. If an individual's visa is revoked,

[15]The Intelligence Reform and Terrorism Prevention Act of 2004, as amended, defines the Information Sharing Environment as "an approach that facilitates the sharing of terrorism and homeland security information, which may include any method determined necessary and appropriate for carrying out [section 1016]." See Pub. L. No. 108-458, § 1016(a)(2), 118 Stat. 3638, 3665 (codified as amended at 6 U.S.C. § 485(a)(3)). See also Homeland Security Act of 2002, 6 U.S.C. § 482 (requiring the establishment of procedures for the sharing of homeland security information, as defined by this section).

under existing procedures, this information is to be entered into the database CBP uses to screen airline passengers prior to their boarding, which we describe below. According to CBP, when the individual checks in for a flight, the on-site CBP Immigration Advisory Program officers already would have been apprised of the visa revocation by CBP and they would have checked the person's travel documents to verify that the individual was a match to the visa revocation record. Once the positive match was established, the officers would have recommended that he not be allowed to board the flight.

Under another scenario, if an individual is on TSC's terrorist screening database, existing processes provide CBP with the opportunity to identify the subject of a watchlist record as part of the checks CBP is to conduct to see if airline passengers are eligible to be admitted into the country. Specifically, for international flights departing to or from the United States (but not for domestic flights), CBP is to receive information on passengers obtained, for example, when their travel document is swiped. CBP is to check this passenger information against a number of databases to see if there are any persons who have immigration violations, criminal histories, or any other reason for being denied entry to the country, in accordance with the agency's mission. According to CBP, when it identifies a U.S. bound passenger who is on the watchlist, it coordinates with other federal agencies to evaluate the totality of available information to see what action is appropriate. In foreign airports where there is a CBP Immigration Advisory Program presence, the information on a watchlisted subject is forwarded by CBP to program officers onsite. The officers would then intercept the subject prior to boarding the aircraft and confirm that the individual is watchlisted, and when appropriate based on the derogatory information, request that the passenger be denied boarding.

In a third scenario, if an individual is on the watchlist and is also placed on the No Fly or Selectee list, when the person checks in for a flight, the individual's identifying information is to be checked against these lists. Individuals matched to the No Fly list are to be denied boarding. If the individual is matched to the Selectee list, the person is to be subject to further screening, which could include physical screening, such as a pat-down. The criteria in general that are used to place someone on either of these two lists include the following:

- Persons who are deemed to be a threat to civil aviation or national security and should be precluded from boarding an aircraft are put on the No Fly list.

- Persons who are deemed to be a threat to civil aviation or national security but do not meet the criteria of the No Fly list are placed on the Selectee list and are to receive additional security screening prior to being permitted to board an aircraft.[16]

The White House Homeland Security Council devised these more stringent sets of criteria for the No Fly and Selectee lists in part because these lists are not intended as investigative or information-gathering tools or tracking mechanisms, and TSA is a screening but not an intelligence agency.[17] Rather, the lists are intended to help ensure the safe transport of passengers and facilitate the flow of commerce. However, the White House's review of the December 25 attempted terrorist attack raised questions about the effectiveness of the criteria, and the President tasked the FBI and TSC with developing recommendations for any needed changes to the nominations guidance and criteria.

Weighing and responding to the potential impacts that changes to the nominations guidance and criteria could have on the traveling public and the airlines will be important considerations in developing such recommendations. In September 2006, we reported that tens of thousands of individuals who had similar names to persons on the watchlist were being misidentified and subjected to additional screening, and in some cases delayed so long as to miss their flights.[18] We also reported that resolving these misidentifications can take time and, therefore, affect air carriers and commerce. If changes in criteria result in more individuals being added to the lists, this could also increase the number of individuals who are misidentified, exacerbating these negative effects. In addition, we

[16]Of all of the screening databases that accept watchlist records, only the No Fly and Selectee lists require certain nomination criteria or inclusion standards that are narrower than the "known or appropriately suspected" standard of HSPD-6. The most recent guidance related to the No Fly and Selectee list criteria was issued in February 2009.

[17]The Homeland Security Council originally was established in 2001 by executive order and subsequently codified into law by the Homeland Security Act of 2002 for the purpose of more effectively coordinating the policies and functions of the federal government relating to homeland security. See Exec. Order No. 13,228; Pub. L. No. 107-296, tit. IX, 116 Stat. 2135, 2258-59 (codified at 6 U.S.C. §§ 491-496). On May 26, 2009, the President announced the full integration of White House staff supporting national security and homeland security into a new "National Security Staff" supporting all White House policy-making activities relating to international, transnational, and homeland security matters. The Homeland Security Council was maintained as the principle venue for interagency deliberations on issues that affect the security of the homeland, such as terrorism, weapons of mass destruction, natural disasters, and pandemic influenza.

[18]GAO-06-1031.

explained that individuals who believe that they have been inappropriately matched to the watchlist can petition the government for action and the relevant agencies must conduct research and work to resolve these issues. If more people are misidentified, more people may trigger this redress process, increasing the need for resources. Finally, any changes to the criteria or process would have to ensure that watchlist records are used in a manner that safeguards legal rights, including freedoms, civil liberties, and information privacy guaranteed by federal law.

## Agencies Do Not Screen Individuals against All Records in the Watchlist, Which Creates Potential Security Vulnerabilities; GAO Continues to Recommend That Agencies Assess and Address These Gaps

In reacting to the December 25 attempted terrorist attack, determining whether there were potential vulnerabilities related to the use of watchlist records when screening—not only individuals who fly into the country but also, for example, those who cross land borders—are important considerations. Screening agencies whose missions most frequently and directly involve interactions with travelers generally do not check against all records in the consolidated terrorist watchlist. In our October 2007 report, we noted that this is because screening against certain records may not be needed to support a respective agency's mission or may not be possible because of computer system limitations, among other things.[19]

For example, CBP's mission is to determine if any traveler is eligible to enter the country or is to be denied entry because of immigration or criminal violations. As such, CBP's computer system accepts all records from the consolidated watchlist database that have either a first name or a last name and one other identifier, such as a date of birth. Therefore, TSC sends CBP the greatest number of records from the consolidated watchlist database for its screening. In contrast, one of the State Department's missions is to approve requests for visas. Since only non-U.S. citizens and nonlawful permanent residents apply for visas, TSC does not send the department records on citizens or lawful permanent residents for screening visa applicants.

Also, the FBI database that state and local law enforcement agencies use for their missions in checking individuals for criminal histories, for example, also receives a smaller portion of the watchlist. According to the FBI, its computer system requires a full first name, last name, and other identifier, typically a date of birth. The FBI noted that this is because having these identifiers helps to reduce the number of times an individual

[19] GAO-08-110.

is misidentified as being someone on the list, and the computer system would not be effective in making matches without this information. Finally, the No Fly and Selectee lists collectively contain the lowest percentage of watchlist records because the remaining ones either do not meet the nominating criteria, as described above, or do not meet system requirements—that is, include full names and dates of birth, which TSA stated are required to minimize misidentifications.

TSA is implementing a new screening program that the agency states will have the capability to screen an individual against the entire watchlist.[20] Under this program, called Secure Flight, TSA will assume from air carriers the responsibility of comparing passenger information against the No Fly and Selectee lists.[21] According to the program's final rule, in general, Secure Flight is to compare passenger information only to the No Fly and Selectee lists.[22] The supplementary information accompanying the rule notes that this will be satisfactory to counter the security threat during normal security circumstances. However, the rule provides that TSA may use the larger set of watchlist records when warranted by security considerations, such as if TSA learns that flights on a particular route may pose increased risks. TSA emphasized that use of the full terrorist screening database is not routine. Rather, TSA noted that its use is limited to circumstances in which there is information concerning an increased risk to transportation security, and the decision to use the full watchlist database will be based on circumstances at the time. According to TSA, as of January 2010, the agency was developing administrative procedures for utilizing the full watchlist when warranted.

In late January 2009, TSA began to assume from airlines the watchlist matching function for a limited number of domestic flights, and has since phased in additional flights and airlines. TSA expects to assume the watchlist matching function for all domestic and international flights departing to and from the United States by December 2010. It is important to note that under the Secure Flight program, TSA requires airlines to provide the agency with each passenger's full name and date of birth to facilitate the watchlist matching process, which should reduce the number

[20]GAO-09-292.

[21]Pub. L. No. 108-458, § 4012(a), 118 Stat. 3638, 3714-15 (codified at 49 U.S.C. § 44903(j)(2)(C)).

[22]See 73 Fed. Reg. 64,018 (Oct. 28, 2008) (codified at 49 C.F.R. pt. 1560).

of individuals who are misidentified as the subject of a watchlist record. We continue to monitor the Secure Flight program at the Congress's request.

In our October 2007 watchlist report, we recommended that the FBI and DHS assess the extent to which security risks exist by not screening against certain watchlist records and what actions, if any, should be taken in response.[23] The agencies generally agreed with our recommendations but noted that the risks related to not screening against all watchlist records needs to be balanced with the impact of screening against all records, especially those records without a full name and other identifiers. For example, more individuals could be misidentified, law enforcement would be put in the position of detaining more individuals until their identities could be resolved, and administrative costs could increase, without knowing what measurable increase in security is achieved. While we acknowledge these tradeoffs and potential impacts, we maintain that assessing whether vulnerabilities exist by not screening against all watchlist records—and if there are ways to limit impacts—is critical and could be a relevant component of the government's ongoing review of the watchlist process. Therefore, we believe that our recommendation continues to have merit.

## Identifying Additional Screening Opportunities and Determining Whether There Are Clear Lines of Authority for and Accountability over the Watchlist Process Would Help Ensure Its Effective Use

As we reported in October 2007, the federal government has made progress in using the consolidated terrorist watchlist for screening purposes, but has additional opportunities to use the list. For example, DHS uses the list to screen employees in some critical infrastructure components of the private sector, including certain individuals who have access to vital areas of nuclear power plants or transport hazardous materials. However, many critical infrastructure components are not using watchlist records, and DHS has not finalized guidelines to support such private sector screening, as HSPD-6 mandated and we previously recommended.[24]

In that same report, we noted that HSPD-11 tasked the Secretary of Homeland Security with coordinating across other federal departments to

[23]GAO-08-110.

[24]The identification of critical infrastructure components that are not using watchlist records for screening is considered Sensitive Security Information that cannot be disclosed in a public statement.

develop (1) a strategy for a comprehensive and coordinated watchlisting and screening approach and (2) a prioritized implementation and investment plan that describes the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of necessary activities.[25] We reported that without such a strategy, the government could not provide accountability and a basis for monitoring to ensure that (1) the intended goals for, and expected results of, terrorist screening are being achieved and (2) use of the watchlist is consistent with privacy and civil liberties. We recommended that DHS develop a current interagency strategy and related plans.

According to DHS's Screening Coordination Office, during the fall of 2007, the office led an interagency effort to provide the President with an updated report, entitled, HSPD-11, An Updated Strategy for Comprehensive Terrorist-Related Screening Procedures.[26] The office noted that the report was formally submitted to the Executive Office of the President through the Homeland Security Council and reviewed by the President on January 25, 2008. Further, the office noted that it also provided a sensitive version of the report to the Congress in October 2008. DHS provided us an excerpt of that report to review, stating that it did not have the authority to share excerpts provided by other agencies, and we were unable to obtain a copy of the full report. The information we reviewed only discussed DHS's own efforts for coordinating watchlist screening across the department. Therefore, we were not able to determine whether the HSPD-11 report submitted to the President addressed all of the components called for in the directive or what action, if any, was taken as a result. We maintain that a comprehensive strategy, as well as related implementation and investment plans, as called for by HSPD-11, continue to be important to ensure effective governmentwide use of the watchlist process.

In addition, in our October 2007 report, we noted that establishing an effective governance structure as part of this strategic approach is particularly vital since numerous agencies and components are involved in

[25]The White House, *Homeland Security Presidential Directive/HSPD-11, Subject: Comprehensive Terrorist-Related Screening Procedures* (Washington, D.C., Aug. 27, 2004).

[26]DHS established the Screening Coordination Office in July 2006 to enhance security measures by integrating the department's terrorist-and immigration-related screening efforts, creating unified screening standards and policies, and developing a single redress process for travelers.

the development, maintenance, and use of the watchlist process, both within and outside of the federal government. Also, establishing a governance structure with clearly-defined responsibility and authority would help to ensure that agency efforts are coordinated, and that the federal government has the means to monitor and analyze the outcomes of such efforts and to address common problems efficiently and effectively. We determined at the time that no such structure was in place and that no existing entity clearly had the requisite authority for addressing interagency issues. We recommended that the Homeland Security Council ensure that a governance structure was in place, but the council did not comment on our recommendation.

At the time of our report, TSC stated that it had a governance board in place, comprised of senior-level agency representatives from numerous departments and agencies. However, we also noted that the board provided guidance concerning issues within TSC's mission and authority. We also stated that while this governance board could be suited to assume more of a leadership role, its authority at that time was limited to TSC-specific issues, and it would need additional authority to provide effective coordination of terrorist-related screening activities and interagency issues governmentwide. In January 2010, the FBI stated that TSC has a Policy Board in place, with representatives from relevant departments and agencies, that reviews and provides input to the government's watchlist policy. The FBI also stated that the policies developed are then sent to the National Security Council Deputies Committee (formerly the Homeland Security Council) for ratification. The FBI noted that this process was used for making the most recent additions and changes to watchlist standards and criteria. We have not yet been able to determine, however, whether the Policy Board has the jurisdiction and authority to resolve issues beyond TSC's purview, such as issues within the intelligence community and in regard to the nominations process, similar to the types of interagency issues the December 25 attempted attack identified. We maintain that a governance structure with the authority for and accountability over the entire watchlist process, from nominations through screening, and across the government is important.

On January 7, 2010, the President tasked the National Security Staff with initiating an interagency review of the watchlist process—including the business processes, procedures, and criteria—and the interoperability and sufficiency of supporting information technology systems. This review offers the government an opportunity to develop an updated strategy, related plans, and governance structure that would provide accountability

to the administration, the Congress, and the American public that the watchlist process is effective at helping to secure the homeland.

## Recent Work Highlights the Importance of Conducting Vulnerability Assessments and Operational Testing Prior to Deployment of New Checkpoint Technologies

### While TSA Has Not Yet Deployed Any New Checkpoint Technologies Nationwide, It Plans to Have Installed Almost 200 AITs by the End of 2010

As we reported in October 2009, in an effort to improve the capability to detect explosives at aviation passenger checkpoints, TSA has 10 passenger screening technologies in various phases of research, development, procurement, and deployment, including the AIT (formerly Whole Body Imager).[27] TSA is evaluating the AIT as an improvement over current screening capabilities of the metal detector and pat-downs specifically to identify nonmetallic threat objects and liquids. The AITs produce an image of a passenger's body that a screener interprets. The image identifies objects, or anomalies, on the outside of the physical body but does not reveal items beneath the surface of the skin, such as implants. TSA plans to procure two types of AIT units: one type uses millimeter wave and the other type uses backscatter X-ray technology. Millimeter wave technology beams millimeter wave radio frequency energy over the body's surface at high speed from two antennas simultaneously as they rotate around the body.[28] The energy reflected back from the body or other objects on the body is used to construct a three-dimensional image. Millimeter wave

[27]GAO-10-128.

[28]According to TSA, this description of the millimeter wave technology applies only to the machine manufactured by L3 and does not apply to other millimeter wave technologies that TSA is evaluating, such as the Smiths millimeter wave AIT.

technology produces an image that resembles a fuzzy photo negative. Backscatter X-ray technology uses a low-level X-ray to create a two-sided image of the person. Backscatter technology produces an image that resembles a chalk etching.[29]

As we reported in October 2009, TSA has not yet deployed any new technologies nationwide. However, as of December 31, 2009, according to a senior TSA official, the agency has deployed 40 of the millimeter wave AITs, and has procured 150 backscatter X-ray units in fiscal year 2009 and estimates that these units will be installed at airports by the end of calendar year 2010. In addition, TSA plans to procure an additional 300 AIT units in fiscal year 2010, some of which will be purchased with funds from the American Recovery and Reinvestment Act of 2009.[30] TSA plans to procure and deploy a total of 878 units at all category X through category IV airports.[31] Full operating capability is expected in fiscal year 2014. TSA officials stated that the cost of the AIT is about $130,000 to $170,000 per unit, excluding installation costs. In addition, the estimated training costs are $50,000 per unit.

While TSA stated that the AIT will enhance its explosives detection capability, because the AIT presents a full body image of a person during the screening process, concerns have been expressed that the image is an invasion of privacy. According to TSA, to protect passenger privacy and ensure anonymity, strict privacy safeguards are built into the procedures for use of the AIT. For example, the officer who assists the passenger never sees the image that the technology produces, and the officer who views the image is remotely located in a secure resolution room and never sees the passenger. Officers evaluating images are not permitted to take cameras, cell phones, or photo-enabled devices into the resolution room. To further protect passengers' privacy, ways have been introduced to blur the passengers' images. The millimeter wave technology blurs all facial features, and the backscatter X-ray technology has an algorithm applied to

[29]Research and development of the AIT technology is continuing, specifically, to develop passive terahertz (THz) and active gigahertz (GHz) technologies to improve detection performance and reduce operational costs of commercially available systems.

[30]According to TSA, some of the 300 AIT units to be procured in fiscal year 2010 will begin to be deployed to airports in the latter half of fiscal year 2010.

[31]TSA classifies the commercial airports in the United States into one of five security risk categories (X, I, II, III, and IV). In general, category X airports have the largest number of passenger boardings, and category IV airports have the smallest. Categories X, I, II, and III airports account for more than 90 percent of the nation's air traffic.

the entire image to protect privacy. Further, TSA has stated that the AIT's capability to store, print, transmit, or save the image will be disabled at the factory before the machines are delivered to airports, and each image is automatically deleted from the system after it is cleared by the remotely located security officer. Once the remotely located officer determines that threat items are not present, that officer communicates wirelessly to the officer assisting the passenger. The passenger may then continue through the security process. Potential threat items are resolved through a direct physical pat-down before the passenger is cleared to enter the sterile area.[32] In addition to privacy concerns, the AITs are large machines, and adding them to the checkpoint areas will require additional space, especially since the operators are segregated from the checkpoint to help ensure passenger privacy.

## TSA Reports That It Is Taking Steps to Operationally Test AITs but Has Not Conducted Vulnerability Assessments

We previously reported on several challenges TSA faces related to the research, development, and deployment of passenger checkpoint screening technologies and made a number of recommendations to improve this process.[33] Two of these recommendations are particularly relevant today, as TSA moves forward with plans to install a total of 878 additional AITs—completing operational testing of technologies in airports prior to using them in day-to-day operations and assessing whether technologies such as the AIT are vulnerable to terrorist countermeasures, such as hiding threat items on various parts of the body to evade detection.

First, in October 2009, we reported that TSA had relied on technologies in day-to-day airport operations that had not been proven to meet their functional requirements through operational testing and evaluation, contrary to TSA's acquisition guidance and a knowledge-based acquisition approach. We also reported that TSA had not operationally tested the AITs at the time of our review, and we recommended that TSA operationally test and evaluate technologies prior to deploying them.[34] In commenting

[32]TSA stated that it continues to evaluate possible display options that include a "stick figure" or "cartoon-like" form to provide greater privacy protection to the individual being screened while still allowing the unit operator or automated detection algorithms to detect possible threats.

[33]GAO-10-128.

[34]Operational testing refers to testing in an operational environment in order to verify that new systems are operationally effective, supportable, and suitable.

on our report, TSA agreed with this recommendation. A senior TSA official stated that although TSA does not yet have a written policy requiring operational testing prior to deployment, TSA is now including in its contracts with vendors that checkpoint screening machines are required to successfully complete laboratory tests as well as operational tests. The test results are then incorporated in the source selection plan. The official also stated that the test results are now required at key decision points by DHS's Investment Review Board. While recently providing GAO with updated information to our October 2009 report, TSA stated that operational testing for the AIT was completed as of the end of calendar year 2009. We are in the process of verifying that TSA has tested all of the AIT's functional requirements in an operational environment.

Deploying technologies that have not successfully completed operational testing and evaluation can lead to cost overruns and underperformance. TSA's procurement guidance provides that testing should be conducted in an operational environment to validate that the system meets all functional requirements before deployment. In addition, our reviews have shown that leading commercial firms follow a knowledge-based approach to major acquisitions and do not proceed with large investments unless the product's design demonstrates its ability to meet functional requirements and be stable.[35] The developer must show that the product can be manufactured within cost, schedule, and quality targets and is reliable before production begins and the system is used in day-to-day operations.

TSA's experience with the ETPs, which the agency uses for secondary screening, demonstrates the importance of testing and evaluation in an operational environment. The ETP detects traces of explosives on a passenger by using puffs of air to dislodge particles from the passenger's body and clothing that the machine analyzes for traces of explosives. TSA procured 207 ETPs and in 2006 deployed 101 ETPs to 36 airports, the first deployment of a checkpoint technology initiated by the agency.[36] TSA deployed the ETPs even though agency officials were aware that tests conducted during 2004 and 2005 on earlier ETP models suggested that they did not demonstrate reliable performance. Furthermore, the ETP

[35]GAO, *Best Practices: Using a Knowledge-Based Approach to Improve Weapon Acquisition*, GAO-04-386SP (Washington, D.C.: January 2004).

[36]TSA deployed the ETPs from January to June 2006. Since June 2006, TSA removed all but 9 ETPs from airports because of maintenance issues.

models that were subsequently deployed were not first tested to prove their effective performance in an operational environment, contrary to TSA's acquisition guidance, which recommends such testing. As a result, TSA procured and deployed ETPs without assurance that they would perform as intended in an operational environment. TSA officials stated that they deployed the machines without resolving these issues to respond quickly to the threat of suicide bombers. In June 2006, TSA halted further deployment of the ETP because of performance, maintenance, and installation issues. According to a senior TSA official, as of December 31, 2009, all but 9 ETPs have been withdrawn from airports and 18 ETPs remain in inventory. TSA estimates that the 9 remaining ETPs will be removed from airports by the end of calendar year 2010. In the future, using validated technologies would enhance TSA's efforts to improve checkpoint security. Furthermore, retaining existing screening procedures until the effectiveness of future technologies has been validated could provide assurances that use of checkpoint technologies improves aviation security.

Second, as we reported in October 2009, TSA does not know whether its explosives detection technologies, such as the AITs, are susceptible to terrorist tactics. Although TSA has obtained information on vulnerabilities at the screening checkpoint, the agency has not assessed vulnerabilities—that is, weaknesses in the system that terrorists could exploit in order to carry out an attack—related to passenger screening technologies, such as AITs, that are currently deployed. According to TSA's threat assessment, terrorists have various techniques for concealing explosives on their persons, as was evident in Mr. Abdulmutallab's attempted attack on December 25, where he concealed an explosive in his underwear. However, TSA has not assessed whether these and other tactics that terrorists could use to evade detection by screening technologies, such as AIT, increase the likelihood that the screening equipment would not detect the hidden weapons or explosives. Thus, without an assessment of the vulnerabilities of checkpoint technologies, it is unclear whether the AIT or other technologies would have been able to detect the weapon Mr. Abdulmutallab used in his attempted attack. TSA is in the process of developing a risk assessment for the airport checkpoints, but the agency has not yet completed this effort or clarified the extent to which this effort addresses any specific vulnerabilities in checkpoint technology.

TSA officials stated that to identify vulnerabilities at airport checkpoints, the agency analyzes information such as the results from its covert testing program. TSA conducts national and local covert tests, whereby individuals attempt to enter the secure area of an airport through the

passenger checkpoint with prohibited items in their carry-on bags or hidden on their persons. However, TSA's covert testing programs do not systematically test passenger and baggage screening technologies nationwide to ensure that they identify the threat objects and materials the technologies are designed to detect, nor do the covert testing programs identify vulnerabilities related to these technologies. We reported in August 2008 that while TSA's local covert testing program attempts to identify test failures that may be caused by screening equipment not working properly or caused by screeners and the screening procedures they follow, the agency's national testing program does not attribute a specific cause of a test failure.[37] We recommended, among other things, that TSA require the documentation of specific causes of all national covert testing failures, including documenting failures related to equipment, in the covert testing database to help TSA better identify areas for improvement. TSA concurred with this recommendation and stated that the agency will expand the covert testing database to document test failures related to screening equipment.

In our 2009 report, we also recommended that the Assistant Secretary for TSA, among other actions, conduct a complete risk assessment—including threat, vulnerability, and consequence assessment—for the passenger screening program and incorporate the results into TSA's program strategy, as appropriate. TSA and DHS concurred with our recommendation, but have not completed these risk assessments or provided documentation to show how they have addressed the concerns raised in our 2009 report regarding the susceptibility of the technology to terrorist tactics.

Mr. Chairman, this concludes our statement for the record.

## Contacts and Acknowledgments

For additional information on this statement, please contact Eileen Larence at (202) 512-6510 or larencee@gao.gov or Stephen Lord at (202) 512-4379 or lords@gao.gov.

[37]See GAO, *Transportation Security: TSA Has Developed a Risk-Based Covert Testing Program, but Could Better Mitigate Aviation Security Vulnerabilities Identified Through Covert Tests*, GAO-08-958 (Washington, D.C.: Aug. 8, 2008).

In addition to the contacts named above, Kathryn Bernet, Carissa Bryant, Frances Cook, Joe Dewechter, Eric Erdman, Richard Hung, Anne Laffoon, Linda Miller, Victoria Miller, and Michelle Woods made key contributions to this statement.

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

## Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548